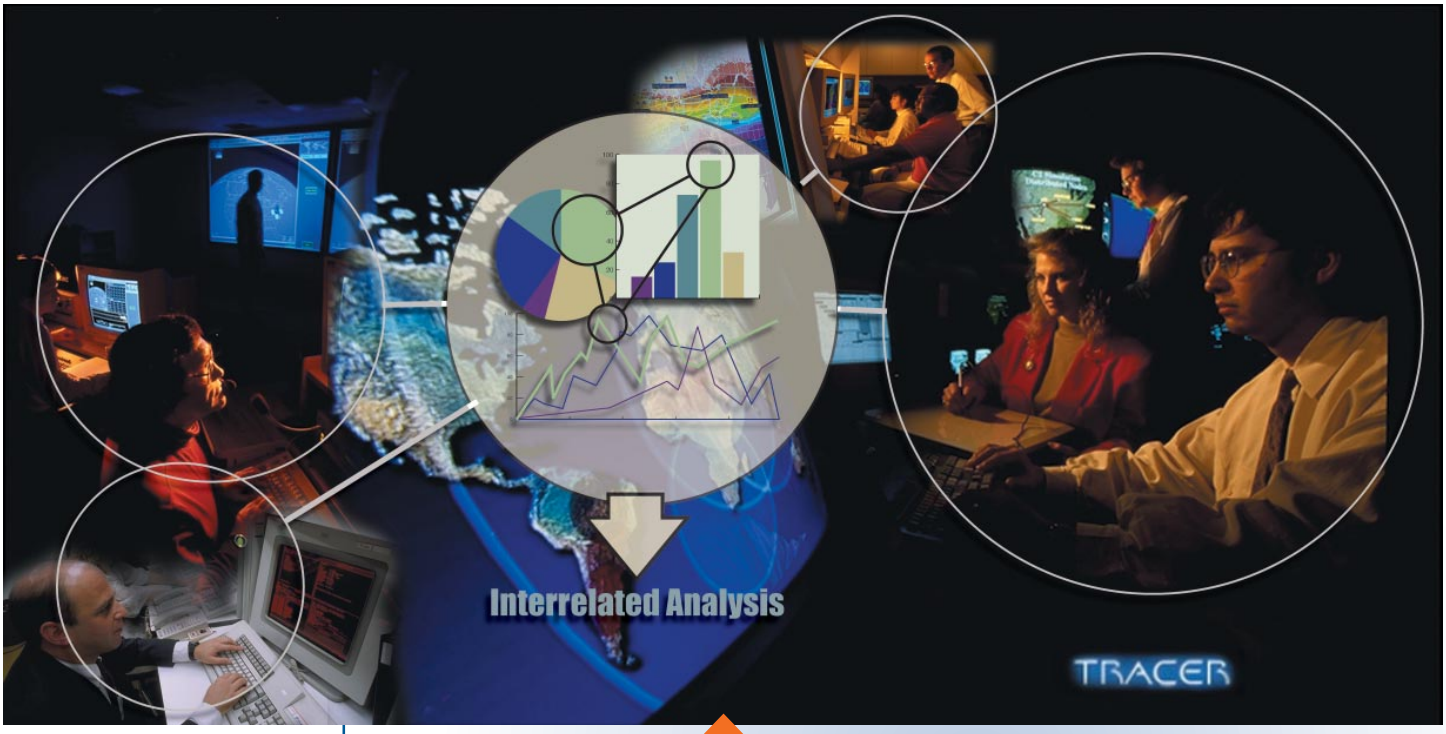


*The heart of the Tracer system is a patent-pending approach to presenting interrelated views of the high-volumes of security data.*

National Security

# Cyber Security Integrated Analysis

*Enterprise Level Security Analysis System*

The challenge to keep one step ahead of the hackers is relentless and all too familiar.

Attackers are constantly adapting and becoming more sophisticated. Tools that worked a year ago are becoming less effective and many can no longer handle the dramatically increased loads. Sensors now generate tens of thousands of records daily and firewall, web and network devices log millions of records each day. While data storage is important, effective analysis is the key.

A highly effective analysis tool must overcome the weaknesses inherent in current approaches.

Additionally, data must be available and accessible. Removing data limits forensic capabilities and inhibits the ability to discover new trends and patterns. Even with data online, a linear method of searching a particular thread may take hours or even days; and all the time, new attacks are being recorded. A new approach will help analysts stay ahead of the game.

### *INL Analysis Tool*

INL computer scientists have developed a web-based database application capable of processing and storing hundreds of millions of sensor and log data records. This application, called Tracer, presents the data in a web browser in a unique and powerful way, allowing the analyst to see trends, patterns, details and hidden relationships.

The system was designed on the premise that the human security expert, armed with appropriate tools to view data is more effective than current automated computer systems in detecting and preventing attacks.

*Continued on back*

Idaho National Laboratory

*Continued from front*

### Analysis Views

The heart of the system is a patent-pending approach to presenting interrelated views of the high-volumes of security data. This analysis framework for holding interrelated views was developed to run within a standard web browser anywhere on the network. These views can be added or removed from the framework at will, and each view provides specific functionality that can stand alone.

For example, a view may include graphs, charts, maps, lists, or detailed record information. Each view may have drill-down capabilities and can be independently expanded as a separate web page.

The power of the system is revealed when these views are combined within the framework and interact. This interaction allows the security analyst to evaluate a variety of displays simultaneously. When he or she finds something of interest, a click on the graph will cause all of the displays to re-query and display specific data related to the items of interest.

### System Features

**Data-driven:** Flexible and adapts dynamically based on table values.

**Unique user profiles:** Allows each security analyst to select those groupings of views on their analysis framework, with the potential for multiple frameworks.

**Auditing:** Customized auditing provides tracking of changes made to records in specific tables in the database. Full auditing of all transactions is also available.

**Filtering and grouping:** Functionality allows sensor data to be filtered without being deleted and to be tagged and grouped based on the analysts needs and requirements.

**Forensic data:** Data generated by sensors and logs are maintained in the system and available for forensics or to support legal or investigative requirements.

**System documentation:** To support need for continual additions and changes, full programming and system documentation is available for reference.

### Architecture

**Hardware/OS:** Running a mid-level Sun server with Solaris 9

**Web Server:** Apache 2.0.48

**Application Server:** Sun Java 2 Enterprise Edition 1.3

**Database:** Oracle 9i

**Client:** Standard web browser

### Why use Tracer?

Key benefits to using Tracer include:

**Cost savings:** There are no licensing fees for federal agencies and other government organizations. The system is also designed for easy installation and customization, reducing initial and on-going costs.

**Flexible and adaptable design:** The system can incorporate new analysis methods and techniques quickly and without rework.

**Increased staff effectiveness:** Better tools will allow current staff to be more productive, lessening the need to hire additional and scarce security experts.

**Open and customizable:** All data structures and code are available and customizable. They can easily be adapted to your specific needs and data sources.

**System and network protection:** The most important benefit to this application is its ability to assist in effectively detecting threats to critical data, systems and networks.


### For more information:

**Dale Christiansen**
208-526-1360
Dale.Christiansen@inl.gov

**Robert Hoffman**
208-526-8599
Robert.Hoffman@inl.gov


***Each view in the Tracer system may have drill-down capabilities and can be independently expanded as a separate web page.***